GeekBrains

Урок 9Тема 1

Поиск бинарных уязвимостей

Реверс-инжиниринг

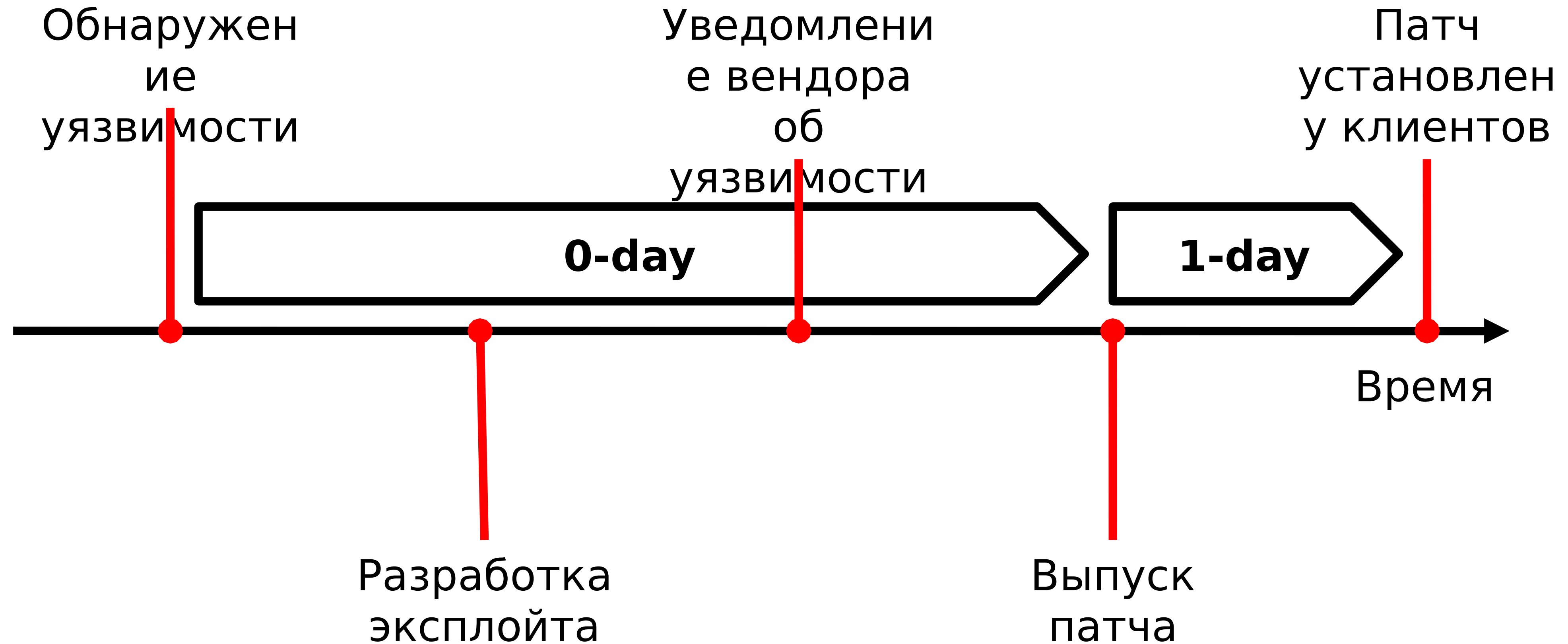
В этом видео

1. Примеры бинарных уязвимостей.
2. Разница между 0-day и 1-day уязвимостями.
3. Способы поиска бинарных уязвимостей.
4. Причины скрытия исправленных уязвимостей.

Примеры бинарных уязвимостей

- Переполнение буфера.
- Целочисленные переполнения.
- Уязвимости формата строки.
- . . .

Разница между уязвимостями 0-day и 1-day



GeekBrains

Способы поиска бинарных уязвимостей

- Фаззинг — 0-day
- Анализ исходного кода — 0-day
- Анализ дизассемблированного кода — 0-day
- Анализ патча — 1-day

Причины и цели скрытия исправленных уязвимостей

- Причины:
  - наличие серьезной уязвимости может повлиять на репутацию вендора;
  - требуется много времени на обновление продукта у клиентов.
- Цели
  - снижение вероятности появления эксплойта в публичном доступе.

GeekBrains

Итоги

1. Узнали, какие уязвимости являются бинарными.
2. Узнали, что такое уязвимости 0-day и 1-day.
3. Познакомились с основными способами поиска бинарных уязвимостей.
4. Поняли, в каких случаях для поиска уязвимостей может быть использован реверс-инжиниринг.